Università degli Studi di Genova

Scuola Politecnica

Dip. di Meccanica, Energetica, Gestionale e dei Trasporti
Dip. di Informatica, Bioingegneria, Robotica e dei Sistemi

Dottorato in Ingegneria Matematica e Simulazione

Resilienza di sistemi Cyber-fisici: valutazione sperimentale di misure quantitative nel contesto della sicurezza informatica

Candidata
Giuseppina MÙRINO

Advisor

Prof. Armando TACCHELLA (DIBRIS)
Prof. Alessandro ARMANDO (DIBRIS)

Co-advisor

Gen.D.A. Francesco VESTITO (CIOC - MINISTERO DIFESA)

Anno Accademico 2018/2019

A Maya e Ludovica,
uniche meravigliose stelle
del mio firmamento

"It is not the strongest of the species that survives,
not the most intelligent that survives.
It is the one that is the most adaptable to change."
Charles Darwin

Sommario

I *sistemi cyber-fisici* (*CPSs*, dall'inglese *Cyber-Physical Systems*) interconnettono il mondo fisico con il mondo digitale allo scopo di automatizzare la produzione e la distribuzione dei processi industriali. Oggigiorno, la maggioranza dei CPSs non operano in maniera isolata (come peraltro accadeva sino a poco tempo addietro) ma, al contrario, la loro componente digitale è connessa in rete per consentire un monitoraggio da remoto attivo, in grado cioè di abilitarne il controllo e la configurazione a distanza. Ogni connessione attiva può offrire facili punti d'accesso ad hackers malevoli permettendo loro di guadagnare, in maniera *silente*, il controllo del sistema e, sfruttando l'accesso al mondo fisico sottostante, provocare, a tempo debito, interruzioni di servizio e/o causare gravi danni all'ambiente circostante. Le misure di prevenzione e monitoraggio, adottabili per la sicurezza delle reti, possono sicuramente ridurre la probabilità di cyber-attacchi ma il rischio residuo d'intrusione rimane comunque inaccettabile laddove gli obiettivi da difendere siano le *Infrastrutture Critiche* (*Critical Infrastructures*) o i *servizi strategici* di uno Stato.
La *resilienza*, intesa come *"la capacità di un sistema di fronteggiare eventi inattesi mantenendo un livello accettabile di operatività"*, è diventata quindi la proprietà chiave per ogni sistema. Obiettivo della presente tesi di dottorato è stata la ricerca di una metodologia di valutazione quantitativa della resilienza, *model-free* e *general-purpose*, che consenta di ottenere indici di resilienza, ad esempio, dai log di sistema o dai dati di processo.
Anche se in letteratura sono già state presentate differenti metriche utilizzabili per la quantificazione della resilienza, poco lavoro è stato sinora fatto in materia di sperimentazione applicativa per la cyber security dei CPSs. Dopo aver realizzato, utilizzando il software Matlab/Simulink®, un modello semplificato (nella sola LINEA ACQUA) di un impianto di trattamento delle acque reflue realmente esistente si è provveduto a simulare attacchi in grado di interferire con il *feedback control loop* critico del sistema per fornire una valutazione della resilienza residua attraverso quattro differenti indici mutuati dall'analisi della letteratura esistente e scelti dopo attenta revisione di oltre quaranta articoli.
I risultati ottenuti mostrano come, nonostante i diversi indici differiscano in termini di comportamento e sensitività, rispetto ai differenti modelli d'attacco testati, ognuno di essi possa sintetizzare ed estrapolare informazioni significative dall'enormità dei log generati dal sistema. La metodologia di valutazione adottata comprende un particolare approccio adottato al fine di estrarre indicatori di performance del sistema dalle variabili di stato osservate che non richiede la conoscenza delle dinamiche del sistema sottostante ed una discussione sull'opportunità di aggregare molteplici indici di resilienza per formulare un'unica misura complessiva di resilienza di sistema.

Ringraziamenti

Un grazie di cuore al Prof. Armando Tacchella ed al Prof. Alessandro Armando (DIBRIS) che, accogliendomi nel loro gruppo di ricerca, hanno consentito la realizzazione di questo ambizioso obiettivo supportandomi e spronandomi con tutte le loro forze

Al Gen. D.A. Francesco Vestito - Comandante del CIOC (Comando Interforze Operazioni Cibernetiche - Ministero della Difesa) tutta la mia stima ed i miei ringraziamenti per il supporto fornito in qualità di Correlatore e l'impegno profuso con il suo eccellente gruppo di lavoro

Alla società Leonardo S.p.A., nelle persone del Dott. Andrea Campora e dell'Ing. Fabio Cocurullo, per il contributo ed l'interesse mostrato nella realizzazione del progetto

Al Prof. Roberto Cianci, nella Sua qualità di Coordinatore del Corso di Dottorato di "Ingegneria delle Macchine e dei Sistemi per l'energia, l'ambiente ed i trasporti", un sincero ringraziamento per la professionalità mostrata durante l'intero percorso

Un ringraziamento speciale a tutti i miei colleghi dell'AIMS LAB che mi hanno accolto nella loro grande Famiglia e con i quali, giorno dopo giorno, ho condiviso gioie e dolori, sacrifici e successi del meraviglioso mondo della ricerca

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

Introduzione

1.1 Contesto

Un *sistema cyber-fisico* (CPS) è definibile come *"an implement intertwining physical processes, hardware, software and communication networks"* [26].
Poche parole per esprimere un concetto di ben ampio respiro che includendo:

- *la presenza di oggetti interconnessi*: i quali, tramite sensori, attuatori ed una connessione di rete, sono in grado di generare e produrre dati di vario genere, riducendo così le distanze e le asimmetrie informative tra i diversi soggetti coinvolti
- *l'attribuzione alla comunicazione di un ruolo di primaria importanza*: grazie alla pervasività, trasversalità e velocità dei dati scambiati i diversi soggetti sono in grado di comunicare in qualsiasi momento e in qualsiasi condizione, fornendo la possibilità di trasformare le grandi moli di dati in informazioni a valore aggiunto
- il concetto di *"Digital Twin"*: ovvero la capacità dicotomica di tali sistemi di creare e affiancare all'aspetto fisico dei prodotti, dei sistemi e dei processi quello virtuale o digitale

ha reso di fatto i CPS una delle innovazioni tecnologiche chiave (*Key Enabling Technology* – KET) della quarta rivoluzione industriale (o *Industry 4.0*).

Gli *Industrial Control System* (ICS) - come *Supervisory Control and data Acquisition* (SCADA), *Distributed Control Systems* (DCS) ed *Programmable Logic Controllers* (PLC) - introdotti dalla terza rivoluzione industriale (Fig. 1.1) per supportare ed efficientare l'attività operativa in ambito industriale e nelle Infrastrutture Critiche, per natura "chiusi" al mondo esterno, sono così stati connessi ad Internet con ineluttabili gravi conseguenze derivanti dalla necessità di integrare il mondo dell'*Operational Technology* (OT), da un lato, con quello dell'*Information Technology* (IT), dall'altro.

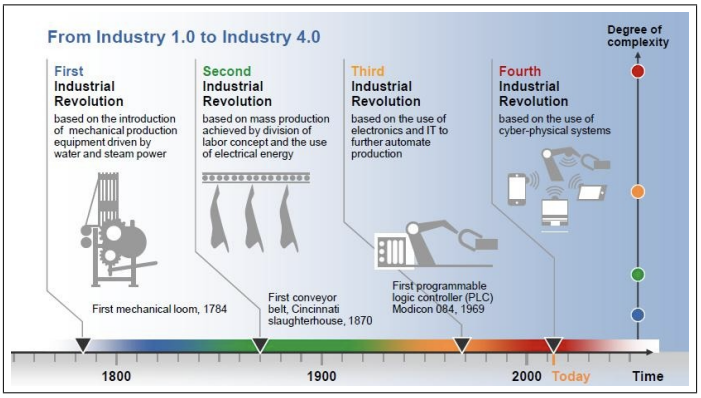

Figura 1.1: Evoluzione dell'industria nei secoli

Due mondi tradizionalmente separati che presentano, peraltro, differenti caratteristiche, esigenze e priorità (Fig. 1.2).

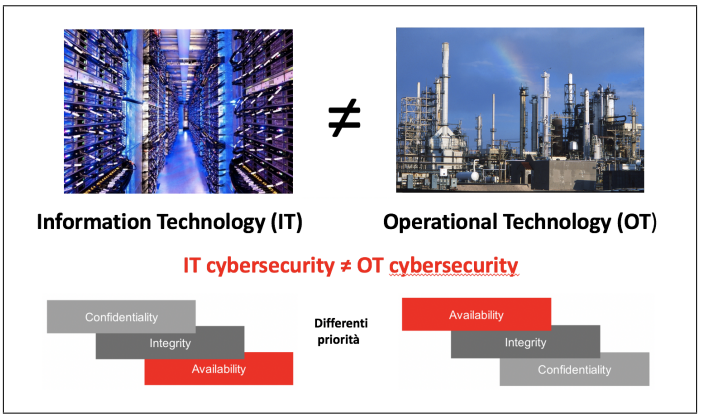

Figura 1.2: *Information technology* vs *Operational technology*

Se nell'IT, infatti, la *Confidentiality* rappresenta il primo dei requisiti da preservare e l'*Availability* è accettato come l'ultimo dei requisiti richiesti in ordine di priorità, nel mondo OT accade l'esatto contrario. La perdita di controllo di un ICS può provocare, infatti, l'interruzione della produzione e generare un grave danno economico ma anche rappresentare una vera e propria catastrofe per la sicurezza nazionale laddove ad essere coinvolte siano le infrastrutture critiche di uno Stato.
La minaccia di attacchi hacker, sino a poco tempo addietro circoscritta al mondo IT, si è così propagata al mondo OT sfruttando proprio il punto di debolezza del sistema rappresentato dal cosiddetto *"red dot"* ovvero dal punto di interconnessione dei due mondi.
Il numero degli incidenti che coinvolgono la sicurezza dei sistemi cyber-fisici è quindi incredibilmente aumentato in questi ultimi anni [27]. L'enorme potenziale distruttivo rappresentato dalla possibilità che un hacker possa prendere il controllo di un'infra-

struttura critica ha attenzionato anche il mondo della Difesa che, coerentemente con scelte adottate nel 2016 dalla Nato, ha necessariamente dovuto ampliare i propri tradizionali quattro domini (*terra, aria, mare e spazio*) ad una nuova quinta dimensione: il *cyberspace*.

In Italia, è stato così istituito a Roma (presso il C4 Difesa) il *Comando Interforze Operazioni Cibernetiche* (CIOC) creato e comandato dal Gen.D.A. Francesco Vestito. In Fig. 1.3 (sotto) è presentato il Quadro Normativo di Riferimento Nazionale costituito sulla base del *DPCM Gentiloni*[1] del 17 febbraio 2017 e dell'aggiornamento del *"Piano Nazionale di protezione cibernetica e la sicurezza informatica"*[2] recanti gli indirizzi strategici per la cyber sicurezza nazionale[3].

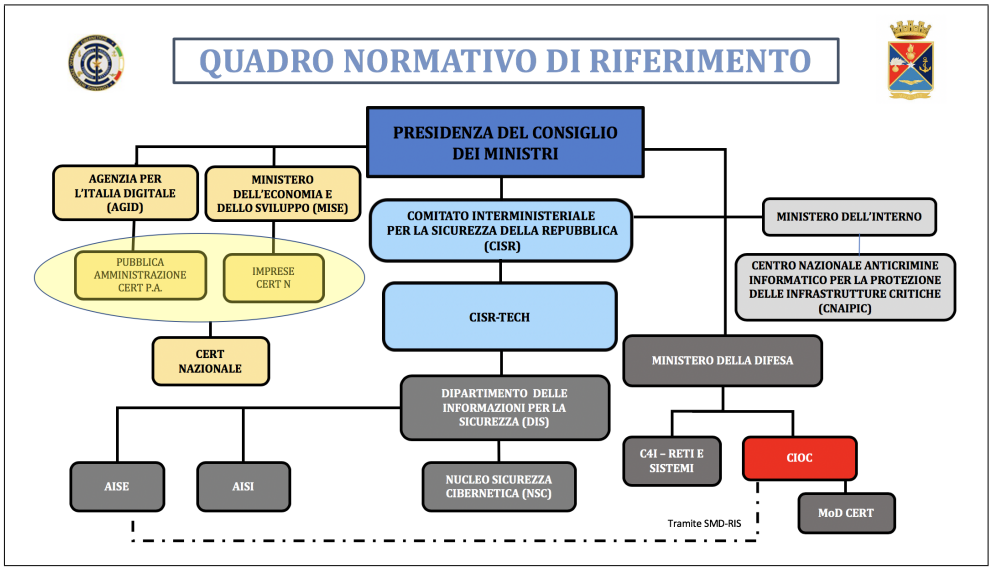

Figura 1.3: La *Cybersecurity* in Italia

1.2 Motivazioni

In questo scenario, molte misure sono state adottate per aumentare la sicurezza dei sistemi cyber-fisici; nuove architetture per gli ICS sono state ideate [40], sistemi più performanti di *monitoring* & *detection* sono stati implementati sulle reti, ma la probabilità di accadimento di eventi inattesi non potrà mai, purtroppo, essere completamente azzerata e le conseguenze correlate al rischio residuo restano sempre troppo pesanti per non cercare di trovare ulteriori soluzioni volte alla sua ulteriore

[1] https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html

[2] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf

[3] https://www.consorzio-cini.it/index.php/it/news-ita/1249-libro-bianco-della-cybersecurity

mitigazione.
Il concetto di *resilienza* già sdoganato nel 2013 dal Presidente Obama nella *Presidential Policy Directive* (PPD-21) ove si definiva: *"resilience as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to* ***withstand and recover from deliberate attacks,*** *accidents, or naturally occurring threats or incidents."* è stato utilizzato per coniare il nuovo termine di *cyber-resilience* intesa come ***"the ability to continously deliver the intended outcome despite adverse cyber events*** [5], accezione nella quale si inquadra perfettamente lo sviluppo della presente ricerca.

Figura 1.4: *Critical Infrastructure* Sectors (fonte DHS)

La necessità di garantire la sicurezza nazionale passa attraverso la tutela della totalità delle Infrastrutture Critiche di ogni Paese. In Fig. 1.4 sono raffigurati i sedici settori che, secondo il *Department Homeland Security*[4] americano, sono riconducibili all'acronimo CI (*Critical Infrastructure*).

A partire dal famoso Aurora generation test del 2007, primo storico attacco hacker condotto, in via sperimentale, dall'Idaho National Lab (USA) per provare al mondo intero[5] come fosse possibile distruggere un generatore da 27 tonnellate con una sequenza di zeri ed uno lanciata a migliaia di chilometri di distanza, peraltro senza possibilità di individuare con certezza l'autore dell'atto terroristico, numerosi eventi

[4] https://www.dhs.gov/science-and-technology/csd-cpssec
[5] https://youtu.be/LM8kLaJ2NDU

si sono verificati nel mondo intero (Fig. 1.5)[6].

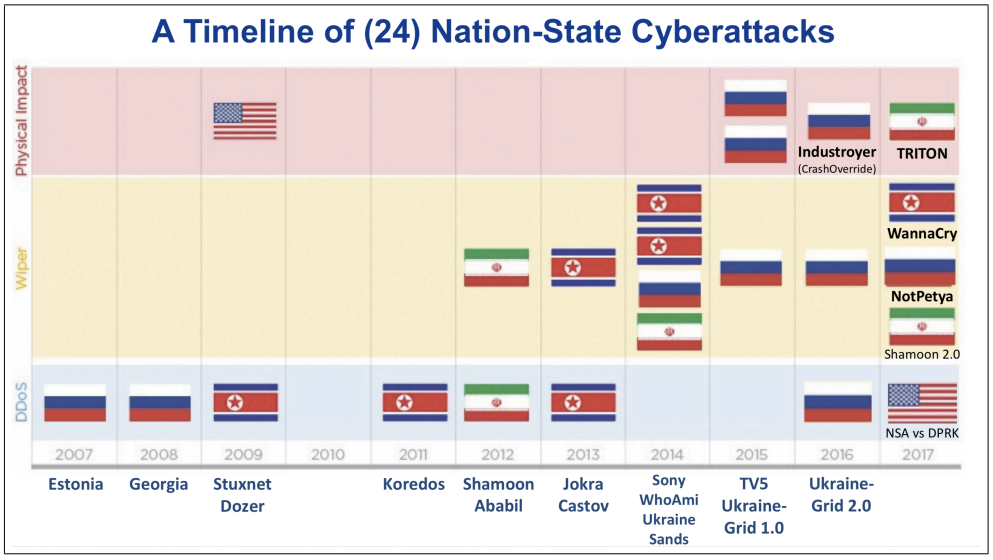

Figura 1.5: Cronologia dei principali cyber attacchi nel mondo

L'ultimo, in ordine di tempo, è noto con il nome di *TRITON* ed è stato perpetrato nei confronti di una raffineria nel Vicino Oriente, con il seguente obiettivo: *"The attack was not designed to simply destroy data or shut down the plant ... It was meant to sabotage the firm's operations and trigger an explosion."* (fonte SANS). Come illustrato in Fig. 1.6, il malware TRITON fornisce un'infrastruttura di attacco costruita per interagire con piattaforme di sicurezza e controllo critico di tipo SIS (*Safety Instrumented System*) a marchio Triconex (Tricon, Trident, Tri-GP), distribuite dalla società Schneider Electric. Un SIS è un sistema autonomo che controlla in modo indipendente lo stato di un processo. Se il processo supera i parametri che definiscono uno stato di pericolo, il SIS tenta di riportare il processo in uno stato sicuro o esegue automaticamente un arresto sicuro del processo (*safe shutdown*). Stando a quanto riportato dagli analisti, gli attaccanti sono riusciti ad introdurre il malware TRITON su una workstation industriale SIS con sistema operativo Windows, mascherandolo come un'applicazione legittima Triconex Trilog, un tool impiegato per controllare i log, parte della suite TriStation. Per poter attivare il payload, TRITON richiede che lo switch a chiave sul pannello posteriore del dispositivo Triconex sia in posizione "PROGRAM" (v. Fig. 1.6). TRITON implementa il protocollo proprietario TriStation, utilizzato per configurare i controller SIS Triconex ed è in grado di comunicare con il SIS, riprogrammandolo con istruzioni definite dall'attaccante o inviandogli specifici comandi per interromperne il funzionamento o leggere il contenuto

[6]https://cyberx-labs.com/resources/sans-webinar-anatomy-of-triton-ics-cyberattack/

della memoria. Nessuna prova evidente che consentisse l'*attribution* dell'attacco è sinora stata trovata.

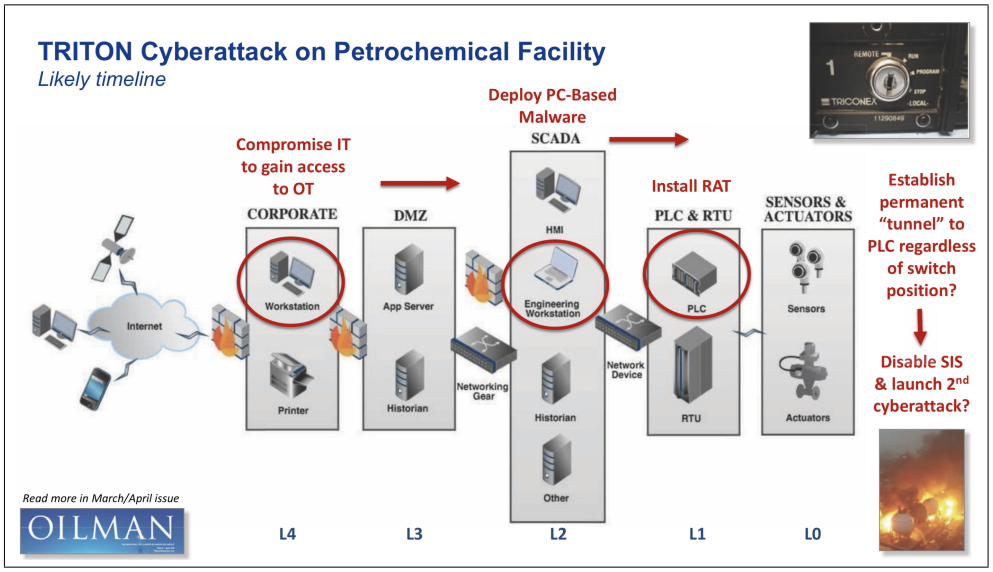

Figura 1.6: Anatomia dell'attacco *Triton*

1.3 Obiettivi

Alla luce di quanto sinora esposto, si è ritenuto che i soggetti direttamente coinvolti nel processo di messa in sicurezza delle infrastrutture critiche nazionali come CERTs (*Computer Emergency Response Team*), organismi di gestione delle crisi cibernetiche, enti regolatori e settori governativi locali e nazionali coinvolti sulla base del Quadro Normativo di Riferimento Nazionale (presentato in Fig. 1.3 (sopra)) potessero essere interessati ad avere a disposizione uno strumento di valutazione della resilienza che presentasse le seguenti proprietà:

1. ***Model free***: stante l'oggettiva difficoltà a costruire e gestire modelli matematici che rappresentino in modo accurato i sistemi cyber fisici reali, la valutazione della resilienza dovrebbe poter prescindere dalla conoscenza precisa delle dinamiche di sistema sottostanti (i.e. sistemi di equazioni differenziali, modelli formali) basandosi, possibilmente, sul solo monitoraggio dei dati di processo e degli eventi

2. ***Quantitative***: dovrebbe poter fornire una misura sintetica di resilienza (o un indice) che descriva, quanto più fedelmente possibile, il grado di danneggiamento che un sistema può tollerare prima di diventare instabile o mostrare comportamenti indesiderati e potenzialmente pericolosi

3. ***General Purpose***: teoricamente, al fine di ottenere economia di scala dalla sua applicazione, la metodologia utilizzata per il calcolo dell'indice di resilienza a partire dagli indicatori di performance del sistema, dovrebbe essere applicabile ad una classe di sistemi quanto più ampia possibile.

1.4 Contributi

Il contributo fornito dalla presente tesi di dottorato consiste nella definizione di una metodologia di valutazione che, rispecchiando fedelmente i requisiti sopra indicati, permetta di estrapolare indici quantitativi di resilienza a partire, ad esempio, da: log di sistema, dati di controllo del processo o log provenienti da un SIEM (*Security Information and Event management*). Al momento, molte delle proposte similari esistenti in letteratura non rispecchiano tali *requirements* e, per quelle che maggiormente si avvicinano alle peculiarità richieste, nessuna evidenza scientifica della loro applicabilità in caso di cyber-attacco è disponibile.

A partire dall'analisi di dettaglio di oltre 47 *research papers* e *surveys* sono stati identificati quattro indici applicabili per quantificare la resilienza indipendentemente dalla conoscenza delle dinamiche e della struttura del sistema. Attraverso un modello realizzato con il software Matlab/Simulink® sulla base dei dati reali di un impianto di trattamento delle acque reflue ed utilizzando il metodo Montecarlo, si è provveduto a simulare (su base giornaliera) differenti ipotesi d'attacco dirette al *feedback control loop* del sistema. I risultati dei differenti indici ottenuti sono stati quindi comparati, sulla base delle differenti ipotesi d'attacco, al fine di individuare l'incidenza dei parametri utilizzati per caratterizzarle (i.e. durata, ampiezza e frequenza).
Il metodo di calcolo degli indici individuato non dipende dalle caratteristiche specifiche del sistema ma è strettamente correlato alla scelta degli indicatori di performance scelti per monitorare la prestazione di sistema attesa. I risultati ottenuti mostrano che, sebbene gli indici analizzati differiscano tra loro in termini di comportamento e sensitività, ognuno di loro è in grado di fornire informazioni significative a partire dalla sola mole di dati di sistema.

Sintetizzando, i contributi offerti dalla ricerca sono pertanto i seguenti:

- comparazione di quattro misure quantitative di resilienza, individuate analizzando oltre 40 lavori di ricerca, in grado di assicurare indipendenza dal modello (*Model Free*) ed ampia applicabilità (*General Purpose*)
- approccio alla quantificazione che non richiede la conoscenza del modello matematico (o formale) delle dinamiche di sistema per estrarre gli indicatori di performance dalle variabili osservate

- una discussione propedeutica all'individuazione di una misura sistematica di resilienza a partire dalla combinazione degli indici ottenuti dalle numerose variabili di stato individuate nel sistema.

1.5 Struttura

Per concludere questo capitolo introduttivo, si presenta, di seguito, la struttura del presente lavoro di tesi.

Capitolo 1 In questa sezione introduttiva si illustrano il contesto e le motivazioni all'interno dei quali è maturata l'idea di sviluppo del progetto di ricerca, si declinano gli obiettivi prefissati ed il valore dei contributi individuati. Infine, si presenta la struttura attraverso la quale la ricerca è presentata.

Capitolo 2 La seconda sezione raccoglie una breve descrizione dello stato dell'arte del principale tema affrontato e dell'utilizzo della modalità di approccio simulativo adottata.

Capitolo 3 Questa sezione raccoglie la descrizione del caso di studio individuato e ne fornisce una sintetica descrizione fisica propedeutica alla comprensione del modello simulativo realizzato e presentato nella sezione successiva.

Capitolo 4 Descrive l'utilizzo proposto della simulazione quale strumento strategico a supporto della valutazione quantitativa della resilienza di un sistema cyber-fisico sottoposto ad attacco hacker. Per il *case study* proposto dopo aver descritto il modello Matlab/Simulink® realizzato, si descrivono in dettaglio i relativi modelli di attacco testati, le modalità di costruzione degli indicatori di performance e gli indici di resilienza utilizzati. A conclusione del capitolo si propone inoltre una discussione sulle modalità d'individuazione di un indice di sistema.

Capitolo 5 In questa sezione, sono presentati i risultati ottenuti dalle prove sperimentali condotte e se ne fornisce un'analisi comparata di dettaglio.

Capitolo 6 La sezione conclusiva è dedicata alla discussione finale dei risultati raggiunti ed all'indicazione delle future linee di ricerca e sviluppo da intraprendere sulla base di quanto emerso dallo studio condotto e nel contesto delle inevitabili variazioni al contorno intervenute al contempo.

Capitolo 2

Stato dell'arte

2.1 Definizioni di resilienza

Il termine *"resilienza"* (dal latino *resilire*) è da sempre comunemente utilizzato per indicare la capacità intrinseca di un individuo o, più in generale, di un sistema di superare le avversità, derivanti da accadimenti inattesi in grado di alterare il naturale svolgersi degli eventi, riorganizzandosi positivamente al fine di ritrovare un nuovo stato di normalità funzionale.

L'applicazione del concetto di resilienza alla ricerca scientifica vede la sua origine nei primi anni Settanta quando, nel settore dell'ecologia, *"resilience was understood as the capacity of an ecosystem to survive, adapt and grow in the face of unforeseen changes"* [20] evidenziando come *"a resilient ecosystem can stay within the stable state when facing a stressor, or can adapt and enter a new stable state - i.e. change the structure while maintaining its functionality - which garantees its existence"*.
L'accettazione di questa prospettiva, basata sull'utilizzo di modelli per il monitoraggio e la gestione dei cambiamenti nell'ecosistema, si è rapidamente diffusa influenzando la ricerca in numerosi altri campi di applicazione [16].
In Fig. 2.1 (sotto), grazie al tool di visualizzazione CiteSpace [9], è stata raffigurata una suddivisione in cluster dei campi di applicazione della resilienza per disciplina.

L'approccio multidisciplinare al concetto di resilienza conseguente all'interazione tra l'individuo e l'ambiente, ha portato a definire *"resilience as the capacity of a system to absorb disturbance and re-organize while undergoing change so as to still retain essentially the same funtion, structure, identity and feedbacks"* [47].
Il passaggio al settore dell'ingegneria è stato guidato da [21] che, definendo come *"engineering systems are designed to provide specified services and should be efficient, continuously working and predictable"*, illustrò la necessità d'intervento dell'uomo, a supporto del ritorno allo stato di stabilità iniziale del sistema, laddove le variazioni intervenute fossero risultate inaccettabili (Fig. 2.2).

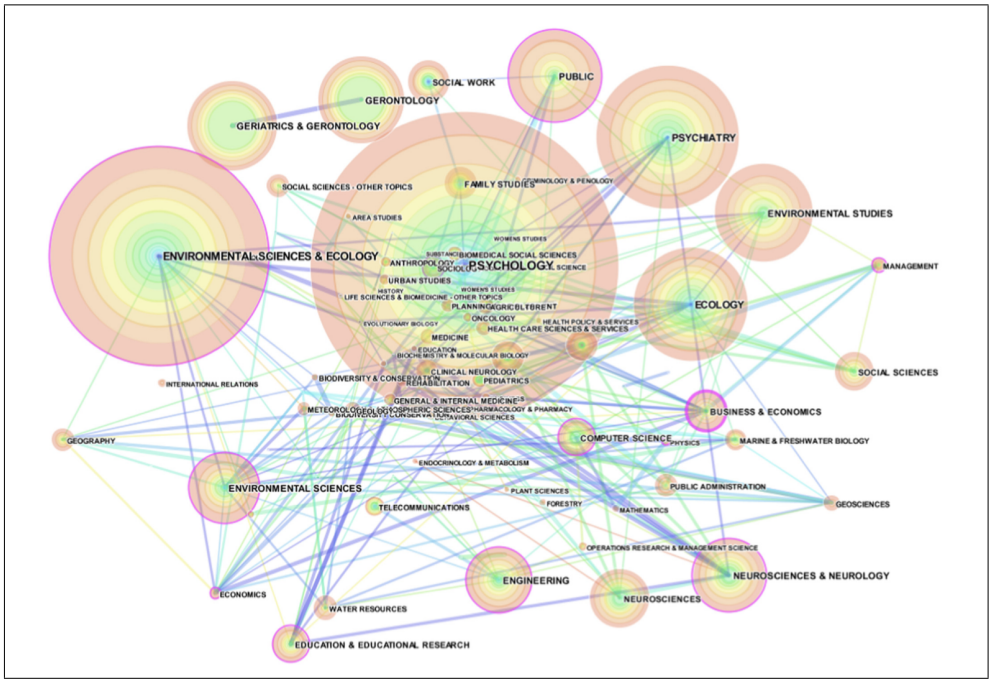

Figura 2.1: Mappa dei cluster disciplinari ottenuta con CiteSpace [23]

Per i sistemi fisici, in particolare, il tema della resilienza è stato quindi ampiamente analizzato negli ultimi decenni, come la copiosa letteratura esistente al riguardo dimostra. Partendo inizialmente dall'ambito *Safety-by-Design*, dove la capacità di adattamento al cambiamento di un sistema deve essere disegnata, la costante crescita in complessità dei sistemi ha portato alla nascita di una vera e propria disciplina nota come *Engineering Resilience* (ovvero *Ingegneria della Resilienza*).
In tempi più recenti, l'avvio della quarta rivoluzione industriale e la conseguente introduzione dei sistemi cyberfisici (CPSs) nell'Industria 4.0 hanno evidenziato la necessità di individuare un nuovo approccio alla valutazione quantitativa della resilienza applicabile sia in ambito *Security-by-Design* quanto in ambito *Safety-by-Retrofit* e molta attività di ricerca si è quindi orientata in questa direzione.
In letteratura, come evidenziato in [18], sono dunque disponibili svariate definizioni di resilienza di un sistema, quali, ad esempio:

- *"Resilience is the ability of a system to absorb external stresses"* [20]
- *"Resilience is a system capability to create foresight, to recognize, to anticipate, and to defend against the changing shape of risk before adverse consequences occur"* [49]
- *"Resilience refers to the inherent ability and adaptive responses of systems that enable them to avoid potential losses"* [43]

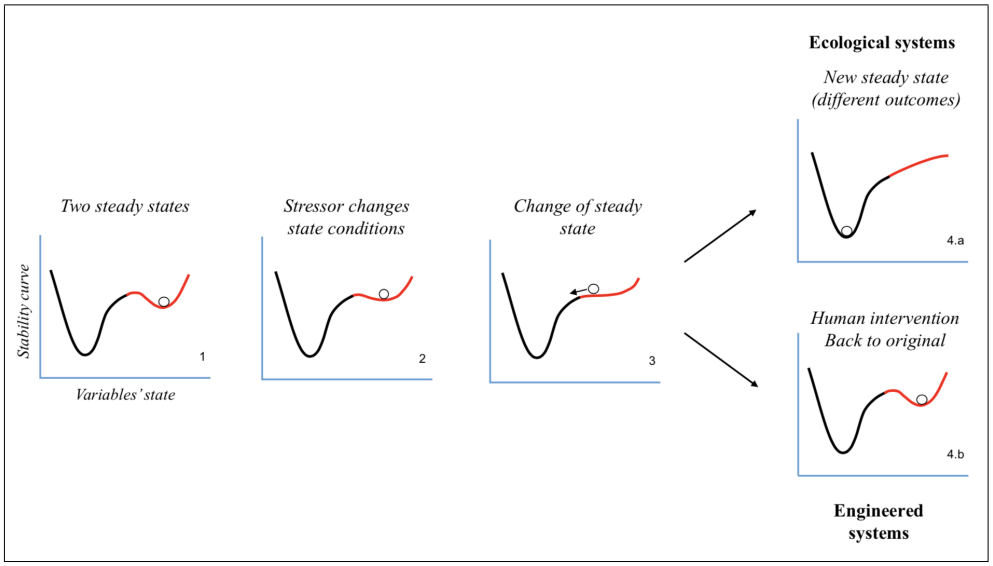

Figura 2.2: Sistema ecologico vs sistema ingegnerizzato [21]

- *"Resilience is the result of a system (i) preventing adverse consequences, (ii) minimizing adverse consequences, and (iii) recovering quickly from adverse consequences"* [48]
- *"Resilience engineering is a paradigm for safety management that focuses on how to help people cope with complexity under pressure to achieve success"* [22]

Nel presente lavoro di tesi, considerato il contesto della ricerca, si è scelto di adottare a riferimento la definizione del termine contenuta nella Presidential Policy Directive 21 (PPD 21 - 2013) [33] di Barack Obama, ovvero:

"The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents"

che, per la prima volta, introduce ed antepone alle possibili minacce tradizionalmente indagate, quali incidenti casuali ed eventi catastrofici naturali, gli *attacchi deliberati* ufficializzando così l'esistenza della minaccia cyber.

2.1.1 La curva di resilienza

Tutte le definizioni, comunque date, non possono prescindere dall'assunto che, per sua stessa natura, la resilienza è intrinsecamente una rappresentazione degli stati del sistema nonchè della loro variazione nel tempo [18].

Un importante strumento utile a supportare la valutazione quantitativa della resilienza è stato individuato in [52] dove, partendo dal presupposto che la resilienza è comunemente associata alla perdita di performance del sistema dopo un evento *"disruptive"*, è stata definita la *curva di resilienza* attraverso la rappresentazione grafica dell'evoluzione nel tempo della curva di performance del sistema *P(t)*. La Fig. 2.3 (sotto), applicando tale concetto, confronta il comportamento di un *sistema resiliente* e di un *sistema non resiliente*, analizzando la performance dei due sistemi conseguente all'accadimento di un evento dirompente inatteso.

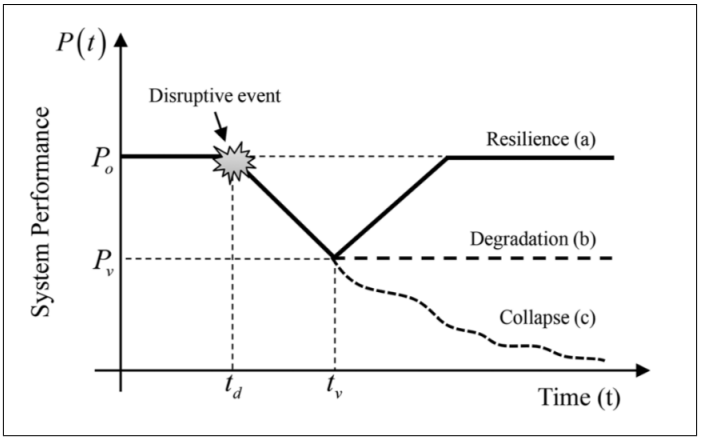

Figura 2.3: *"Sistema resiliente"* vs *"Sistema non resiliente"* [52]

Come si può notare, dopo la perturbazione avvenuta al tempo t_d il *sistema resiliente* (Fig. 2.3 (a)), al tempo t_v, ritorna al livello di performance iniziale P_o mentre il *"sistema non resiliente"*, a seconda delle sue capacità intrinseche, potrebbe di fatto assestare la sua operatività su un livello di performance degradata P_v (Fig. 2.3 (b)) ovvero continuare a degradare il suo livello operativo progressivamente fino al collasso totale (Fig. 2.3 (c)).

In generale, come evidenziato in Fig. 2.4 (sotto), il grafico della *curva di resilienza* è caratterizzato dai seguenti quattro differenti stati:

1. ***Reliability state*** **(S_I)**: che rappresenta lo *stato originale di performance* P_o ovvero la *"baseline" performance* di riferimento del sistema

2. ***Unreliability state*** **(S_{II})**: che rappresenta lo *stato di incertezza o inaffidabilità* del sistema conseguente all'evento *"disruptive"* intervenuto al tempo t_d che ha determinato il raggiungimento, al tempo t_v, del livello di performance degradato P_v

3. ***Recovery state*** **(S_{III})**: che rappresenta lo *stato di ripristino o recupero*, intercorrente tra il tempo t_v ed il tempo t_n, nel quale il sistema, grazie alle sue capacità di recupero, ritorna al livello di performance originale (P_o)

4. ***Recovered steady state*** **(S_{IV})**: che rappresenta, infine, l'avvenuto ritorno del sistema allo *stato di operatività in regime stazionario*, con lo stesso livello di performance iniziale (P_o)

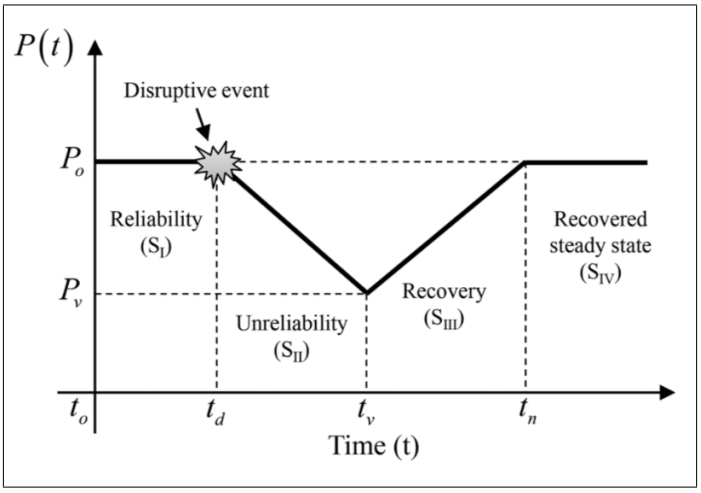

Figura 2.4: I quattro stati della curva di resilienza [52]

Nella realtà, tuttavia, il grafico sopra presentato non risulta essere completamente esaustivo rispetto a tutte le possibili configurazioni che la curva di resilienza può effettivamente assumere.
In Fig. 2.5 (sotto) sono presentate alcune significative variazioni di profilo le cui differenze sono strettamente legate soprattutto allo stato di collasso e di recupero conseguenti all'evento perturbante.
Dopo l'evento inatteso, infatti, l'andamento grafico della curva di resilienza in S_{II} è strettamente correlato alla *severità d'impatto* dell'evento sul livello di performance iniziale P_o. La misura di tale impatto è ottenuta calcolando la differenza tra il livello originale di performance ed il livello raggiunto dopo l'evento (P_o - P_v). Il profilo assunto dalla curva nel periodo di incertezza (tra t_d e t_v) ed il grado di inaffidabilità corrispondente all'angolo θ dipendono tanto dal livello dell'impatto quanto dalla capacità del sistema di reagire al disturbo intervenuto.
Nel grafico presentato sono evidenziati tre differenti profili (u_1, u_2, u_3) cui corrispondono differenti valori dell'angolo θ associato. Nel primo caso, il profilo u_1 assume una direzione ortogonale all'asse t (con angolo $\theta = 0°$) ed identifica lo scenario più pericoloso ovvero quello nel quale il sistema, non risultando in grado di fronteggiare in alcun modo l'evento, collassa immediatamente in maniera irreversibile.
Il secondo profilo u_2 mostra, invece, una graduale perdita di performance del siste-

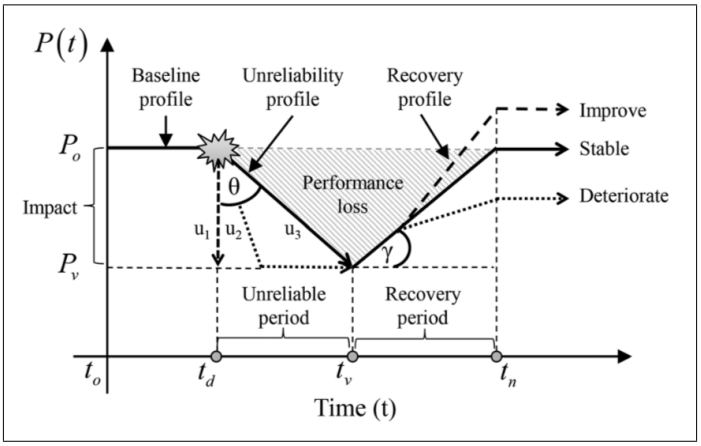

Figura 2.5: Varianti di una generica curva di resilienza [1][2]

ma che si stabilizza sul livello degradato P_v ove persiste prima di iniziare la fase di recupero. In [19][38][15], questo particolare scenario è identificato in un quinto stato del sistema noto come *stato perturbato o degradato*. In tal caso, come mostrato in Fig. 2.6 (sotto), il grafico della *curva di resilienza* risulterà quindi caratterizzato dai seguenti cinque differenti stati:

1. ***Reliability state*** **(S_I)**
2. ***Unreliability state*** **(S_{II})**
3. ***Disrupted state*** **(S_{III})**
4. ***Recovery state*** **(S_{IV})**
5. ***Recovered steady state*** **(S_V)**.

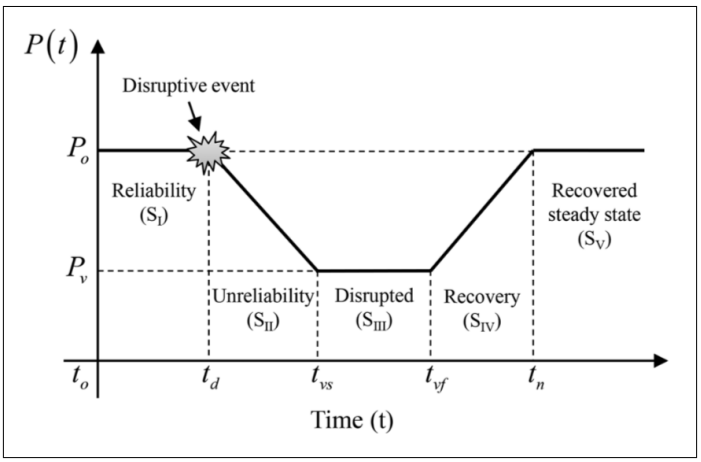

Figura 2.6: I cinque stati della curva di resilienza [19][38][15]

Infine, il terzo profilo u_3 identifica un graduale declino della performance del sistema che raggiunto P_v comincia immediatamente l'azione di recupero. Tale profilo è decisamente preferibile al precedente u_2 in quanto evidenzia una maggiore capacità di reazione del sistema che trova riscontro, dal punto di vista analitico, nel fatto che essendo $\theta u_3 > \theta u_2$, l'area di *Performance Loss (PL)* di u_3 risulta più piccola rispetto a quella di u_2, sebbene in entrambi i casi l'azione di recupero inizi allo stesso istante di tempo t_v .

Il grado di recupero del sistema è, invece, rappresentato dall'angolo γ compreso tra la retta P_v e la curva di resilienza in S_{III} (v. Fig. 2.5).
Anche in questo caso sono stati individuati tre possibili differenti profili cui corrispondono altrettanti scenari di recupero della performance da parte del sistema.
Il primo profilo (*deteriorate*) si riferisce al caso meno favorevole nel quale il sistema non risulta in grado di ritornare al livello di performance originale ma, al contrario, si stabilizza su un livello di performance operativa inferiore (che potrebbe essere ritenuto comunque accettabile o meno).
Il secondo profilo (*stable*) rappresenta il caso auspicabile nel quale il sistema è sufficientemente resiliente da riportarsi autonomamente sul livello di performance iniziale.
Nel terzo profilo (*improve*) il sistema si stabilizza su un livello di performance migliorato rispetto all'originale. In quest'ultimo caso andrebbe poi valutata l'opportunità di mantenimento di tale livello.

Si noti che, complessivamente, l'angolo θ cresce quindi in maniera direttamente proporzionale alla capacità di resilienza del sistema all'impatto dell'evento dirompente (nella fase S_{II}) e l'angolo γ alla capacità di recupero del sistema (nella fase S_{III}).

OSSERVAZIONE: Tutti i profili della curva di resilienza nelle fasi S_{II} ed S_{III} sono stati presentati per semplicità lineari. Nella realtà, in entrambe le fasi, la curva di resilienza può assumere profili concavi, convessi o comunque non lineari, come mostrato (per la sola fase S_{III}) in Fig. 2.7 (sotto).

Un'ulteriore definizione di resilienza, mutuata dalla PPD-21, che integra quanto sinora esposto è la seguente:

"Resilience notionally means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. The resilience of a system's function can be measured based on the persistence of a corresponding functional performance under uncertainty in the face of disturbances"

presentata in [1] sottolineando la sua consistenza anche con la definizione di *rischio* fornita dalla ISO 31010:2009 Risk management - Risk assessment techniques [1], ovvero: *"Risk is the*

[1]International Organization of Standardizations (ISO). Risk Management—Risk Assessment

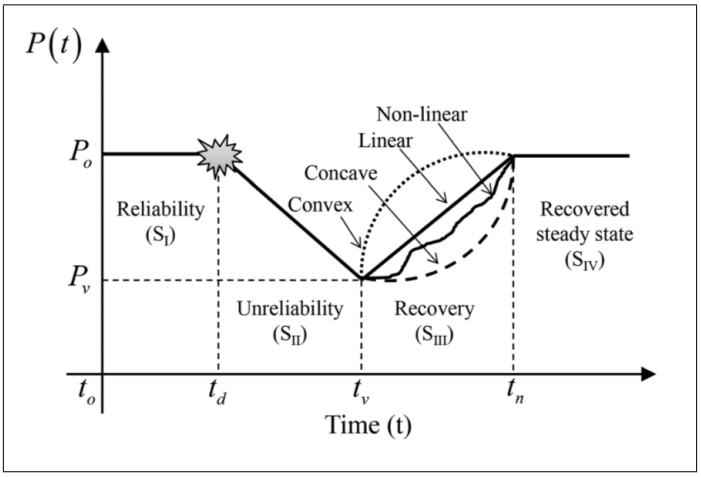

Figura 2.7: Differenti topologie del profilo di ripristino [32]

effect of uncertainty on objectives and an effect is a positive or negative deviation from what is expected".

2.1.2 Il triangolo della resilienza

Un'altro interessante strumento utilizzabile per la valutazione quantitativa della resilienza è presentato in [17] dove, a partire dall'individuazione delle tre *capacità di resilienza* fondamentali, è stato costruito il *triangolo della resilienza* illustrato in Fig. 2.8.

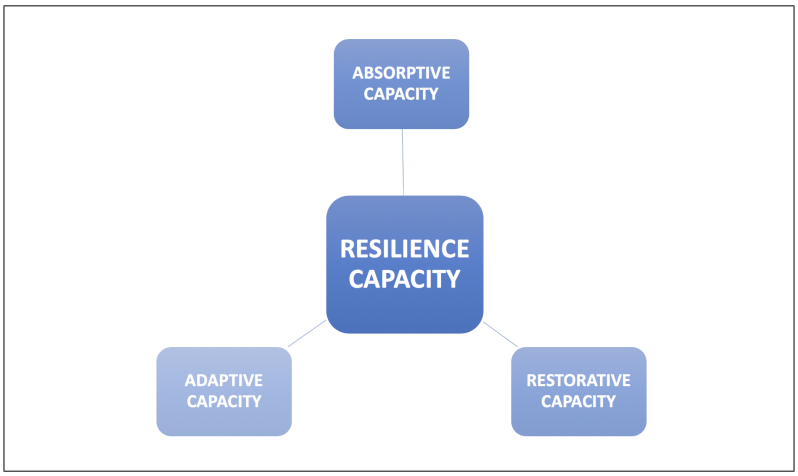

Figura 2.8: Il triangolo della resilienza [17]

I vertici del triangolo risultano essere costituiti da:

Techniques, ISO Standard IEC/FDIS 31010, iso.org, Geneva, Switzerland, 2009.

1. ***Absorptive capacity***: che rappresenta la *capacità di assorbimento* del sistema all'impatto, derivante dalla perturbazione, minimizzando lo sforzo necessario a fronteggiarne le conseguenze [46]
2. ***Adaptive capacity***: che rappresenta la *capacità di adattamento* del sistema ovvero la sua capacità di correzione delle situazioni indesiderabili che possono verificarsi nelle fasi di transizione
3. ***Recovery/Restorative capacity***: che rappresenta, infine, la *capacità di recupero ed aggiustamento* del sistema caratterizzata dalla rapidità con la quale il sistema ritrova un normale o accettabile livello di affidabilità nella gestione operativa.

2.1.3 Quadro di valutazione della resilienza di sistema

Indipendentemento dall'utilizzo finale per il quale è stato progettato, un sistema ingegnerizzato è, per sua natura, una combinazione di componenti fisici che lavorano sinergicamente allo scopo di raggiungere un determinato obiettivo funzionale. Come tale quindi, ogni sistema potrà essere rappresentato come un insieme di variabili con una particolare struttura e proprie peculiari relazioni.

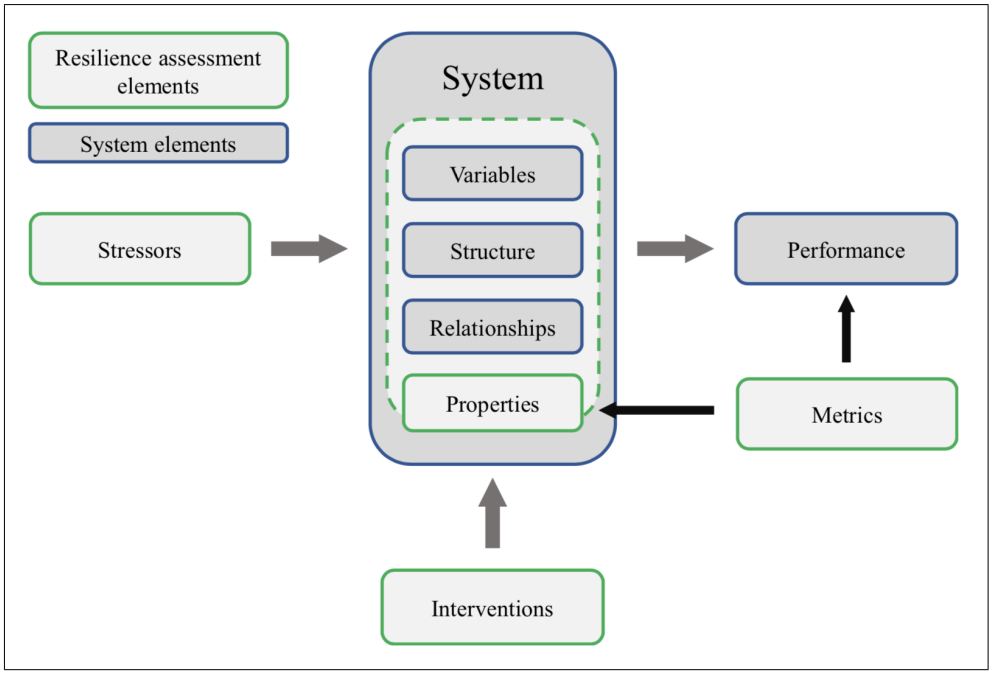

Figura 2.9: Schema concettuale per la valutazione della resilienza di sistema [24]

Lo schema concettuale per la valutazione della resilienza, proposto in [24] e raffigurato in Fig. 2.9 (sopra), identifica i seguenti quattro elementi chiave:

1. ***Stressors***: sono i *fattori di stress* ovvero le *cause scatenanti* che impattando le variabili di sistema producono alterazione nel livello di performance operativa dello stesso.

Se da un lato i fattori cronici (*chronic stressors*) sono ricorrenti, ben noti e possono essere stimati (i.e. invecchiamento delle componenti d'impianto), dall'altro i fattori acuti (*acute stressors*) sono inusuali, imprevedibili e possono avere conseguenze devastanti come nel caso di terremoti, alluvioni o attacchi terroristici.

2. ***Properties***: sono le *proprietà* del sistema che intervengono a supporto della continuità operativa quali, ad esempio: *robustness* (robustezza), *redundancy* (ridondanza), *resourcefulness* (ingegnosità), *flexibility* (flessibilità), *rapidity* (rapidità). Queste proprietà possono essere considerate indicatori di resilienza e quantificate, mediante utilizzo di opportune metriche, sia dal punto di vista quantitativo che qualitativo [51].
3. ***Metrics***: sono gli *indicatori di prestazione*, correlati al livello di performance o di servizio del sistema, utilizzati nella valutazione della resilienza (i.e. *recovery time* (tempo di recupero), *failure magnitude* (grado o livello di guasto)).
4. ***Interventions***: sono gli *interventi* che possono essere adottati per migliorare le proprietà del sistema, a supporto della performance complessiva (i.e.inserimento di sensori di controllo real-time, componenti di riserva, ecc).

L'esigenza di identificare un *framework* per la valutazione della resilienza, evidenziata dai numerosi studi condotti sui sistemi fisici, diventa imprescindibile passando ad analizzare i sistemi cyber-fisici. In questo caso, infatti, il rischio associato all'attacco cyber portato all'infrastruttura non dipenderà solamente dalla resilienza del sistema ma anche dal tipo e dal livello di sofisticazione dell'attacco.

2.1.4 Il Paradigma delle quattro Rs

Le attività di ricerca sulla resilienza in conseguenza di eventi sismici, svolte dalla comunità scientifica di riferimento, hanno portato all'identificazione di quattro particolari proprietà sulle quali focalizzare l'attenzione:

1. ***Robusteness*** ovvero l'abilità di un sistema e degli elementi di un sistema di sopportare perturbazioni esterne senza perdita significativa di performance
2. ***Redudancy*** intesa come la misura con la quale il sistema ed i suoi elementi soddisfano e sostengono i requisiti funzionali in caso di disturbo
3. ***Resourcefulness*** ovvero l'abilità di diagnosticare e prioritizzare i problemi, ovvero di attivare soluzioni attraverso l'identificazione ed il monitoraggio di tutte le risorse (ivi comprese le informazioni economiche, tecniche e sociali)
4. ***Rapidity*** ovvero l'abilità di contenere le perdite di performance, recuperare nonchè evitare future disfunzioni

sistematicamente racchiuse nel cosiddetto *"Paradigma della quattro Rs"* [1].

2.1.5 Figure-Of-Merit (FOM) del sistema

Un importante supporto al calcolo della resilienza di un sistema è l'individuazione di una funzione di transizione in grado di fornire una mappatura, nel tempo, dallo *spazio delle*

variabili di stato del sistema allo *spazio delle prestazioni* del sistema stesso.
Tale funzione, simboleggiata con F(•), è nota in letteratura [19] come *Figure-Of-Merit (FOM)* o *system delivery function* del sistema.

Partendo dall'analisi di un generico sistema d'interesse ***S***, è possibile distinguere tre possibili *stati*:

1. ***Original state*** **($\mathbf{S_0}$)**
2. ***Disrupted state*** **($\mathbf{S_d}$)**
3. ***Recovered state*** **($\mathbf{S_f}$)**

e due transizioni:

1. ***System Disruption***: dall'*Original state* al *Disrupted state*
2. ***System Recovery***: dal *Disrupted state* al *Recovered state*

Due gli eventi che attivano lo schema di transizione raffigurato in Fig. 2.10 (sotto): un *Disruptive Event* ed una *Resilience Action*.
Il primo (che può essere dovuto a fattori interni e/o esterni) attiva la transizione del sistema dallo stato S_0 allo stato S_d. Successivamente il secondo, innescando il processo di recupero, attiva la seconda transizione dallo stato S_d allo stato S_f.

Si noti che, analogamente a quanto descritto nella curva di resilienza, lo stato recuperato S_f può coincidere o meno con lo stato di stabilità iniziale S_0.

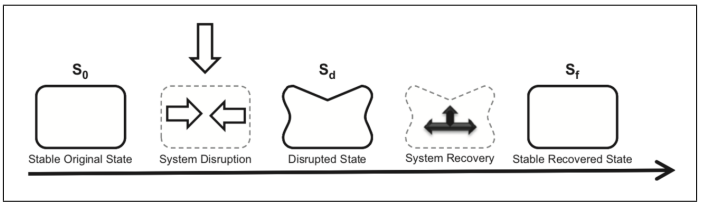

Figura 2.10: Schema di transizione degli stati di sistema nel processi di valutazione della resilienza [19]

Ovviamente, ad ogni stato del sistema S corrisponde un valore della funzione F(•), calcolata secondo la schematizzazione presentata in Fig. 2.11. Tali valori sono strettamente correlati all'occorrenza dei due eventi di attivazione sopra enunciati.

In Fig. 2.12 è presentata la corrispondenza dello schema di transizione degli stati del sistema, illustrato in Fig. 2.10 (sopra), secondo la funzione di mappatura in Fig. 2.11.
Quanto sopra illustrato ha valenza per le *Figure-Of-Merit* nelle quali i valori crescenti sono considerati auspicabili (i.e. flusso, capacità, etc.).
Qualora, al contrario, i valori decrescenti siano da ritenersi preferibili (i.e. percorso più corto), dovrà allora essere considerata la seguente: $G(\bullet) = F(\bullet)^{-1}$.

OSSERVAZIONE: Si noti come la curva $F(t)$ identificata in Fig. 2.12 (sotto) corrisponda di fatto alla curva di resilienza identificata in Fig. 2.6 del paragrafo 2.1.1.

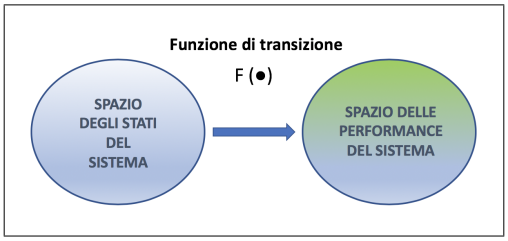

Figura 2.11: Schema di funzionamento della funzione di mappatura F(•)

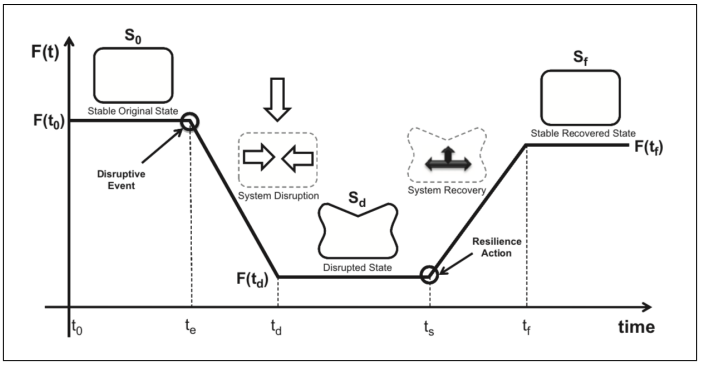

Figura 2.12: Schema concettuale per la valutazione della resilienza di sistema attraverso la funzione di mappatura [19]

2.1.6 Scala di resilienza

Prima di procedere all'analisi delle differenti misure di resilienza proposte in letteratura è opportuno definire la scala metrica di riferimento utilizzata per la loro quantificazione.
La *scala di resilienza* è lo strumento che consente, infatti, di poter quantificare il guadagno o la perdita di resilienza del sistema in maniera univoca. L'utilizzo della scala, infatti, consente il confronto dei valori di resilienza del sistema *pre* e *post-disruption* e permette di individuare il cambiamento subito dal sistema a seguito della perturbazione.
Individuare una scala *universale* di riferimento porterebbe, inoltre, un duplice vantaggio. Da un lato, consentirebbe di semplificare le complicazioni derivanti dall'utilizzo di scale differenti nel confronto dei molteplici indici individuati attraverso l'analisi di sistemi e contesti svariati; dall'altro consentirebbe, una volta individuato il valore della resilienza, di poterlo attribuire al sistema indipendentemente dalla modalità di approccio sulla quale si è basata la sua quantificazione.
Al momento, la maggior parte degli indici espressi in letteratura è basata sulla scala ricompresa tra 0 e 1 ovvero sulla scala percentuale tra 0% e 100%.
L'ipotesi di uniformare la scelta alla prima delle due scale trova ragionevole supporto all'interno della comunità scientifica in ragione del fatto che, essendo l'incertezza una componente importante nell'analisi della resilienza, gli approcci probabilistici hanno valori di probabilità già ricompresi in una scala tra 0 e 1.
L'analisi della resilienza di sistema può svolgere un ruolo fondamentale nella *security-by-retrofit* a supporto della fase di riprogettazione del sistema stesso. Molte sono le possibili cause *disruptive* ed il loro diverso livello di severità può inficiare la capacità di resilienza, per uno stesso sistema, in maniera differente. L'utilizzo di uno strumento di supporto alla

valutazione della resilienza più efficace si tradurrebbe quindi, immediatamente, in una riprogettazione più efficiente a tutto vantaggio dell'implementazione della stessa resilienza di sistema.

2.2 Misure di resilienza

Come illustrato in [23] e sinteticamente schematizzato in Fig. 2.13 (sotto), esistono due differenti modalità di approccio alla valutazione della resilienza di un sistema:

- ***Qualitative Assessment***: che utilizza strumenti di valutazione *qualitativa* basati sul paradigma "interpretativo" e, pertanto, essenzialmente privi di descrittori numerici. Comprende:
  - ***Conceptual Frameworks***: che identificano e schematizzano le *best practices* da seguire nel processo di valutazione
  - ***Semi-quantitative Indeces***: ovvero indici non univocamente definibili ma, tuttavia, utili nelle classificazioni e categorizzazione dei dati analizzati
- ***Quantitative Assessment***: che, contrariamente al caso precedente, utilizza strumenti di valutazione *quantitativa* quali la statistica descrittiva e l'analisi implicativa, per fornire classificazioni e categorizzazioni univoche dei dati analizzati. In questo caso si distinguono due macro sottocategorie:
  - ***General Measures***: che identificano strumenti di misurazione della performance, indipendenti dalla struttura del sistema, attraverso i due seguenti differenti approcci:
    - ***Deterministic Approach***: basato su dati ed eventi assunti in modo *deterministico*
    - ***Probabilistic Approach***: che, al contrario, partendo dalla *stocasticità* di comportamento dei sistemi reali, considera l'*aleatorietà* di dati ed eventi
  - ***Structural-based models***: che, invece, esaminano l'impatto della struttura del sistema sulla resilienza attraverso tre differenti possibili modalità di costruzione dello specifico modello applicativo:
    - ***Optimization Models***: costruzione del *modello matematico* rappresentativo del caso di studio individuato
    - ***Simulation models***: costruzione, attraverso l'utilizzo di tools informatici dedicati, di *modelli di simulazione* del sistema fisico reale (più o meno sofisticati) per analizzarne le dinamiche in tempo reale
    - ***Fuzzy logic models***: costruzione di modelli *fuzzy logic*

Il presente lavoro di tesi è focalizzato all'individuazione ed all'analisi delle misure generali *quantitative* di resilienza del sistema (*Deterministic Approach*) attraverso la costruzione di un modello simulativo realizzato utilizzando il software Matlab/Simulink® .

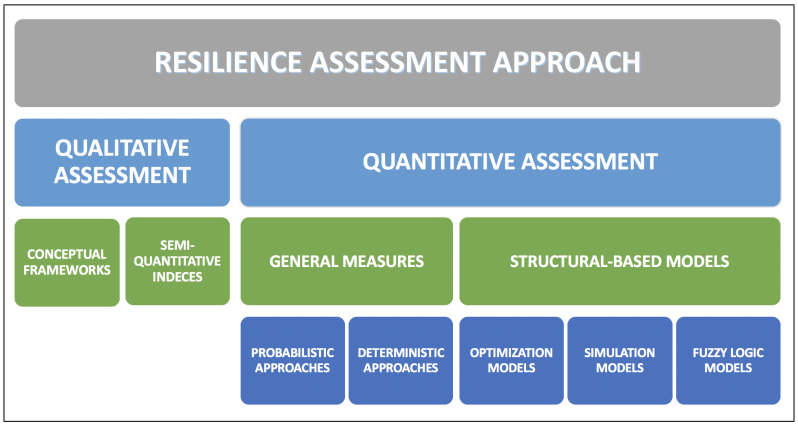

Figura 2.13: *Classificazione delle metodologie di valutazione della resilienza* [23]

2.2.1 Misure quantitative di resilienza

La definizione di misure quantitative di resilienza riveste un ruolo strategico sia nella fase di valutazione della resilienza di un sistema quanto, ancor prima, nella sua implementazione in fase progettuale. L'individuazione univoca di tali misure rappresenta, purtroppo, una sfida ancora aperta; nonostante la ricerca abbia sinora prodotto differenti risultati, infatti, il livello di stardardizzazione è ancora molto basso.
Di seguito una sintesi, non esaustiva, delle misure generiche di resilienza presenti in letteratura raccolte sulla base dei fattori utilizzati per il loro calcolo.

Misure basate sulla curva di resilienza

La curva di resilienza, descritta inella sottosezione 2.1.1, è stata spesso utilizzata dai ricercatori per illustrare il comportamento resiliente di un sistema dopo un evento *disruptive*. Per questo motivo, molte misure di resilienza sono state individuate a partire dall'analisi delle proprietà che tale curva individua. L'area di maggior interesse, corrispondente alla zona ombreggiata in Fig. 2.5 (sopra) e Fig. 2.14 (sotto), (dove è denotata come *Impacted Area (IA)*), è quella che definisce la perdita di performance del sistema conseguente al *disruptive event* occorso al tempo t_d.

In [6], la perdita di resilienza del sistema (ψ_{loss}) è identificata con la perdita di performance e quantificata dalla magnitudine della perdita di performance prevista nel tempo di controllo ($T = t_n - t_d$) secondo la seguente equazione:

$$\psi_{\text{loss}} = \int_{t_{\text{d}}}^{t_{\text{n}}} \left[P_0\left(t_0\right) - P\left(t\right)\right] dt \tag{2.1}$$

dove $P_0\left(t_0\right)$ corrisponde al livello di performance iniziale (nel periodo antecedente il *disruptive event*, ovvero tra t_0 e t_{d}) mentre $P\left(t\right)$ indica la variazione del livello di performance nel tempo successivo.

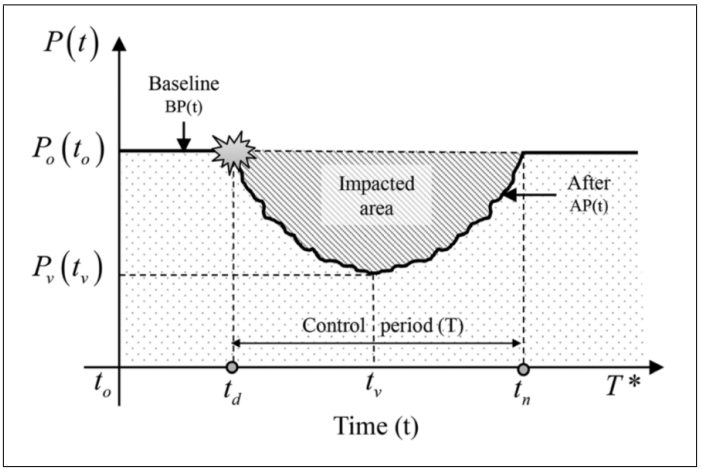

Figura 2.14: Perdita di performance del sistema

Non sempre, fortunatamente, il livello di performance del sistema crolla, immediatamente dopo l'evento dirompente, in direzione ortogonale all'asse del tempo come nel caso del profilo u_1 (con angolo $\theta = 0$) mostrato in Fig. 2.5. Al contrario, in molti casi il profilo della performance del sistema degrada e risale in maniera graduale esibendo, tuttavia, il comportamento non lineare sopra illustrato.
In tal caso, la resilienza del sistema può essere spiegata come la *capacità funzionale* del sistema a seguito della perturbazione nel periodo di controllo ($T = t_\mathrm{n} - t_\mathrm{d}$).
Matematicamente la resilienza ψ può essere quantificata, quindi, sulla base della seguente equazione [41]:

$$\psi = \int_{t_\mathrm{d}}^{t_\mathrm{n}} \frac{AP(t)}{T}\, dt \tag{2.2}$$

come la regione normalizzata sottostante alla curva $AP(t)$ che descrive la funzionalità del sistema dopo l'evento di perturbazione.

Un altro modo per quantificare la resilienza, adottato da numerosi autori [15][38][45], è basato sull'analisi del rapporto tra l'area sottostante la curva di performance del sistema dopo l'evento *disruptive* ($AP(t)$) e la *baseline* o curva di performance iniziale ($BP(t)$), valutate nell'intero periodo di osservazione (compreso tra t_0 e T^*). La relativa equazione:

$$\psi = \frac{\int_{t_0}^{T^*} AP(t)\, dt}{\int_{t_0}^{T^*} BP(t)\, dt} \tag{2.3}$$

è altresì nota come ***"resilienza integrale"***[15].
Si noti che in caso di normalizzazione della *baseline* (considerando cioè che $BP(t)$ assuma

valore costante unitario, ovvero che la performance di base corrisponda al 100% del valore di performance attribuibile) il denominatore della (2.3) risulterà pari a T^* e nel caso specifico, dunque, tale equazione potrebbe essere ricondotta alla (2.2).

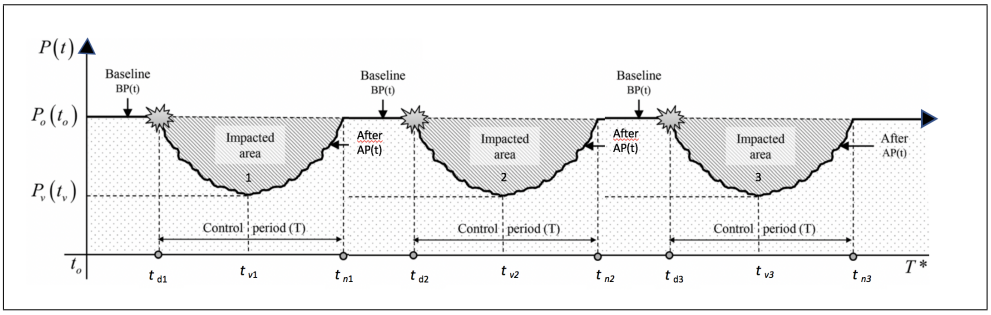

Figura 2.15: Perdita di performance del sistema

Il valore dell'integrale di $AP(t)$ può essere quantificato come differenza tra l'integrale della *baseline* $BP(t)$ e la perdita di performance individuata dalla *Impacted Area (IA)*. Nell'ipotesi che gli eventi di perturbazione si ripetano più volte nell'intervallo di tempo tra t_0 e T^*, come nel caso in Fig. 2.15 (sopra), l'equazione (2.3) è stata riformulata in [36][37] secondo la seguente:

$$\psi = \frac{\int_{t_0}^{T^*} BP(t)\ dt - \sum_{i=1}^{N(T^*)} IA_{\mathrm{i}}(t_{\mathrm{i}})}{\int_{t_0}^{T^*} BP(t)\ dt} \tag{2.4}$$

dove $N(T^*)$ è il numero degli eventi che si verificano nel tempo T^*, i è il numero dell'evento occorso e $IA_i(t_i)$ corrisponde all'*Impacted Area* causata dall'i-esimo evento al tempo t_i.

Un'altra prospettiva di valutazione per la quantificazione della resilienza basata sulla curva di resilienza è fornita in [32] dove, studiando la supply chain, non si analizza solo la *Performance Loss* quale parametro di riferimento per quantificare la resilienza del sistema nel suo complesso ma, al contrario, sono individuate le seguenti ***"5 dimensioni della resilienza"***:

1. ***Recovery***: che definisce il *tempo di recupero* ovvero il tempo necessario al sistema per ritrovare un livello di performance operativa accettabile
2. ***Impact***: che indica la gravità d'impatto dell'evento sulla performance
3. ***Performance Loss***: che identifica l'area ombreggiata, già discussa in precedenza, sottostante alla curva $p(t)$ tra t_1 e t_2
4. ***Profile Length***: ovvero la lunghezza del profilo di recupero tra t_1 e t_2
5. ***Weighted-Sum***: ovvero la misura pesata nel tempo dello scostamento del profilo reale dal profilo lineare di recupero, a seconda della sua concavità o convessità.

In Fig. 2.16 (sotto) sono graficamente illustrate tutte le dimensioni individuate affiancate dalla relativa equazione che le definisce analiticamente. (N.B. La linea tratteggiata individua un

livello di performance p_1 pari al 95% della performance totale; tale valore è stato individuato, nello studio citato, quale livello di performance minimo accettabile *pre* e *post-disruption*).

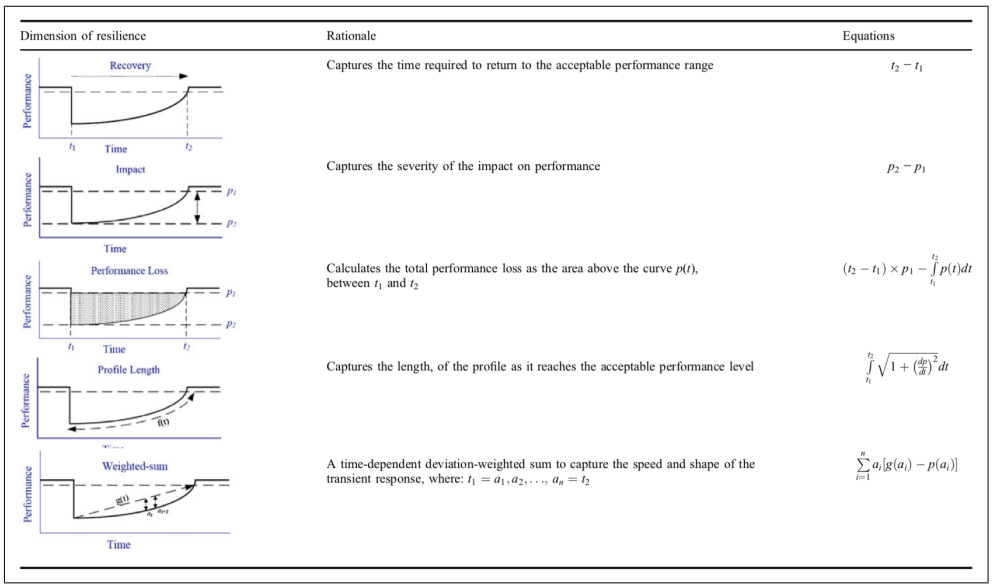

Figura 2.16: Le 5 dimensioni della resilienza [32]

Una formula per la quantificazione della resilienza basata sulle cinque dimensioni sopra illustrate è data dalla seguente equazione:

$$\psi = w_1(Recovery) + w_2(Impact) + w_3(PerformanceLoss) + w_4(ProfileLength) + w_5(Weighted - Sum) \tag{2.5}$$

nella quale $w_1, w_2, ..., w_5$ sono i pesi attribuiti alle singole dimensioni individuati sulla base del modello strutturale indagato.

Misure basate sulla performance *pre* e *post-disruption*

Uno degli approcci più classici alla quantificazione della resilienza dopo un *disruptive event* è basato sulla misura del cambiamento della performance di sistema ottenuta confrontando i valori rilevati nel momento precedente (*pre*) ed in quello successivo (*post*) all'accadimento. La misura della performance è noto essere, per sua stessa natura, strettamente correlata al sistema in analisi e spesso, per uno stesso sistema, può essere espressa attraverso differenti funzioni.
Così, analizzando un sistema interconnesso in rete (i.e. rete di trasporto, rete elettrica o di telecomunicazione), in [34] ad esempio, si é considerato il valore del flusso di veicoli nel sistema quale funzione di performance di riferimento ed individuata la seguente misura di resilienza:

$$\psi = \frac{V_{initial} - V_{loss}}{V_{initial}} \tag{2.6}$$

dove $V_{initial}$ rappresenta, nella fattispecie, il numero massimo di veicoli che possono fruire della rete in condizioni normali (senza incidere sui tempi di percorrenza) e V_{loss} è il numero dei veicoli che non potranno più accedervi a causa dell'evento.

Analogamente, sempre analizzando una rete interconnessa di trasporto in [4], considerando quale funzione di performance il costo associato al tempo di percorrenza della rete per una determinata domanda, è proposta la seguente misura di resilienza normalizzata sul *tempo critico di percorrenza del sistema* (STT)[2]:

$$\psi = \frac{STT - SO}{STT} \tag{2.7}$$

dove SO rappresenta il *tempo ideale di percorrenza del sistema*. E' facile osservare che il numeratore si annulla quando il tempo ideale di percorrenza cresce fino al tempo critico ed in tal caso la resilienza del sistema è praticamente nulla. Viceversa, il sistema è resiliente quando il tempo ideale di percorrenza è molto piccolo e quindi $\psi \simeq 1$.

In generale, il peggior scenario possibile dopo un *disruptive event* è rappresentato dalla perdita totale di performance del sistema, corrispondente al *Max drop* evidenziato in Fig. 2.17. Partendo proprio dall'analisi del caso peggiore, in [42], è stato presentato un indice basato sulla relazione tra l'ulteriore possibile perdita di performance evitata (individuata come *Avoided drop* in Fig. 2.17) e la possibile perdita totale, matematicamente espresso dalla seguente:

$$\psi = \frac{Avoided\ drop}{Max\ drop} = \frac{P_v(t_v) - P_{max}}{P_0(t_0) - P_{max}} \tag{2.8}$$

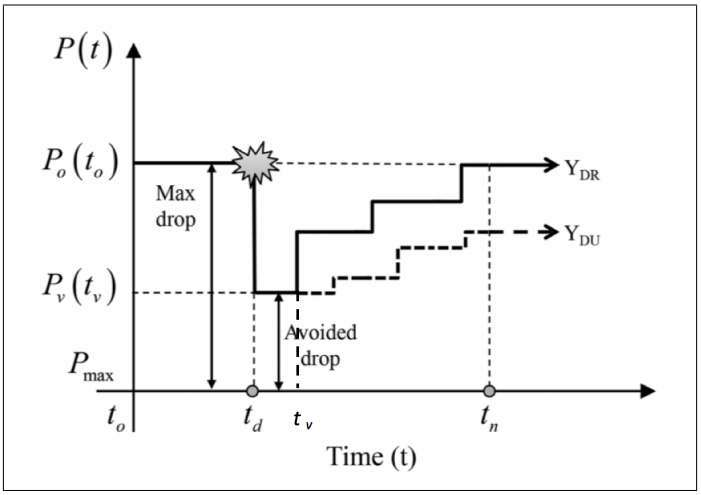

Figura 2.17: *Max* e *avoided drop* dopo un evento *disruptive* [42]

[2]ovvero il massimo costo (di tempo) sopportabile associato ad una grave congestione di traffico nella rete per una determinata domanda di afflusso di veicoli

Nello stesso scenario di analisi della resilienza sotto l'aspetto economico, quando il salto di performance è quantificato sulla percentuale di cambiamento di performance piuttosto che sul valore di performance in output, in [12], l'equazione 2.8 diventa equivalente alla:

$$\psi = \frac{\%\Delta DY^m - \%\Delta DY}{\%\Delta DY^m} \tag{2.9}$$

nella quale $\%\Delta DY^m$ rappresenta la massima variazione percentuale ammissibile in output a seguito dell'evento dirompente e $\%\Delta DY$ la variazione percentuale stimata.
Si noti che in questo secondo caso, si tratta di una misura *statica* di resilienza, ovvero di una misura indipendente dal tempo come illustrato in Fig. 2.18 (sotto).

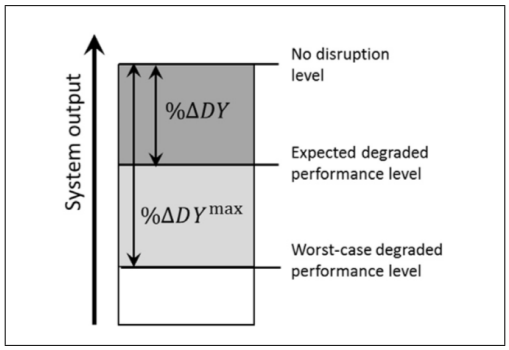

Figura 2.18: Misura *statica* di resilienza [42]

Nei cambiamenti che intercorrono a seguito di un evento destabilizzante, un ruolo importante nella quantificazione della resilienza è svolto dalla *Recovery Performance* ovvero dalla modalità di recupero o ripristino del sistema (nello stato S_{III} di Fig. 2.4). E' evidenza che, a parità di altre condizioni, un sistema più resiliente recupera in maniera più rapida. Così, in [42], facendo riferimento alle due differenti modalità di recupero del sistema identificate con Y_{DR} e Y_{DU} in Fig. 2.17, è presentata la seguente misura di resilienza:

$$\psi = \sum_{t=t_d}^{n} Y_{DR} - \sum_{t=t_d}^{m} Y_{DU} \tag{2.10}$$

dove Y_{DR} è il profilo di recupero resiliente e Y_{DU} è la normale condizione di recupero del sistema mentre m e n sono i tempi di recupero necessari (con $m > n$ a dimostrare uno scenario nel quale tempi inferiori sono richiesti per recuperare sotto un profilo di reazione resiliente).
N.B.: Si osservi che in questo caso, contrariamente a quanto accaduto sinora per le altre metriche individuate, il sistema risulterà resiliente quando $\sum_{t=t_d}^{n} Y_{DU} = \sum_{t=t_d}^{m} Y_{DR}$ ovvero con valore $\psi = 0$ e viceversa non mostrerà resilienza per $Y_{DU} \simeq P_v(t_v)$ tra t_d e t_n ovvero nel caso in cui il sistema non dimostri più capacità di recupero.

Cercando di valutare la resilienza del sistema sanitario ospedaliero nel post-sisma e considerando il tempo atteso in coda dai pazienti per ricevere le cure come indice della qualità del servizio, in [10] la resilienza è stata valutata in termini di qualità del servizio *pre* e *post-disruption* secondo la seguente:

$$\psi = \alpha \int_{t_d}^{t_n} \frac{P_{before}(t)}{T} dt + (1-\alpha) \int_{t_d}^{t_n} \frac{P_{after}(t)}{T} dt \tag{2.11}$$

dove α rappresenta il fattore di peso che rappresenta l'importanza della qualità del servizio prima e dopo l'evento, $P_{before}(t)$ e $P_{after}(t)$ le rispettive performance qualitative del servizio erogato e $T = (t_n - t_d)$ il tempo di controllo del sistema.

Si evidenzia che, nonostante nel lavoro citato si dettagli l'importante ruolo delle ***4 proprietà della resilienza***, (descritte nel *"Paradigma delle quattro Rs"* in 2.1.4), nessuna di esse è stata esplicitamente inserita nell'equazione 2.11, lasciando la misura proposta estremamente dipendente dalla sola scelta del fattore di peso affidata alla discrezionalità dei decision makers.

Misure basate su *Reliability* e *Restoration*

Come ampiamento discusso in precedenza, *Reliability* e *Restoration* sono due attributi essenziali della resilienza.
La prima quantifica, infatti, l'abilità del sistema di mantenere capacità e performance entro un limite di sicurezza predefinito, per un certo periodo di tempo, sotto determinate condizioni; la seconda misura l'abilità di un sistema di ritrovare capacità e performance individuando, prevedendo, mitigando e recuperando gli effetti prodotti da eventi *disruptive* imprevisti.
Diverse formule matematiche sono state identificate in letteratura, quindi, per quantificare la resilienza di un sistema partendo dall'analisi di questi attributi. La maggior parte di esse è calcolata su base probabilistica integrando spesso, a supporto della quantificazione, la probabilità condizionale di raggiungimento di due standard di performance, già descritti in precedenza, ovvero *Robustness* e *Rapidity*.
L'accezione utilizzata per tali standard in [8], ad esempio, identifica la prima come la massima perdita di performance accettabile per il sistema e la seconda come il tempo minimo di interruzione accettabile ovvero il massimo tempo consentito per il suo completo recupero.
In Fig. 2.19 (sotto) è presentata una possibile configurazione di valori assunti da tali standard, proposta nel lavoro citato, a supporto della quantificazione della resilienza di sistema urbano in caso di terremoto.
Il confronto tra lo scenario auspicato e lo scenario ipotizzato si basa su metodo di valutazione *pre* e *post-disruption* probabilistico.

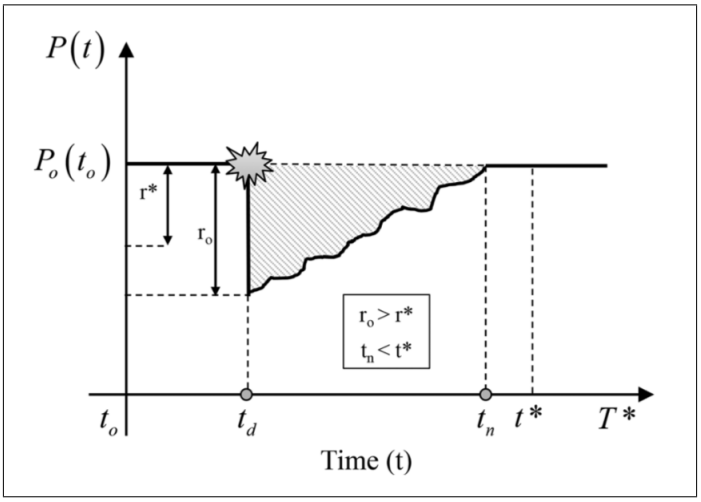

Figura 2.19: *Robustness (r*)* e *Rapidity (t*) auspicate vs valori assunti (r_0, t_n)* [8]

Misure basate su *Vulnerability* e *Recoverability*

Un approccio deterministico per l'individuazione di una misura dinamica di resilienza è proposto in [3] dove, partendo dalla quantificazione della resilienza secondo la seguente:

$$\psi(t) = \frac{Recovery\ (t)}{Loss\ (t)} \tag{2.12}$$

ed utilizzando i tre stati delle Figure-Of-Merit (presentati nella sottosezione 2.1.5) si identifica (v. Fig. 2.20) la *system service function* $\varphi(t)$ che descrive il comportamento o la performance di sistema nel tempo utilizzabile, ad esempio, per descrivere il flusso di traffico ferroviario o la capacità produttiva di uno stabilimento.
In particolare, dato $e^j \in D$, possibile evento *disruptive* all'interno di un insieme di possibili eventi in grado di perturbare lo stato originale del sistema S_0, si definisce il relativo valore di resilienza all'istante di tempo t_r secondo la seguente formula:

$$\psi(t_r|e^j) = \frac{\varphi(t_r|e^j) - \varphi(t_d|e^j)}{\varphi(t_0) - \varphi(t_d|e^j)} \qquad t_r \in (t_s, t_f) \tag{2.13}$$

A partire da tale equazione, gli autori hanno identificato, inoltre, una *Component Importance Measure (CIM)* basata sulla resilienza.
Queste misure, in grado di individuare quali componenti di un sistema sono sostanzialmente più critiche di altre in termini di affidabilità del sistema, sono state generalmente calcolate sulla affidabilità in base al rapporto tra l'apporto della singola componente all'affidabilità del sistema e l'affidabilità complessiva del sistema stesso.
Il carattere della resilienza di sistema identificata nell'equazione 2.13 permette, isolando la *i-esima* componente, di identificare il contributo della componente stessa alla resilienza complessiva di sistema.

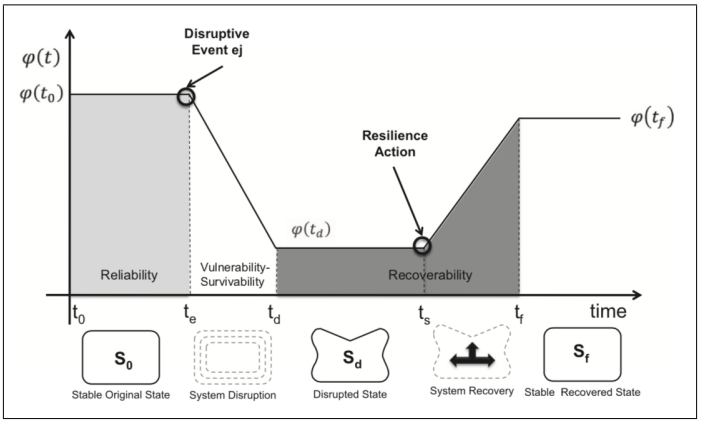

Figura 2.20: Descrizione degli stati di transizione nel tempo in termini di *system service function* [3]

Misure basate sul *"Paradigma delle quattro Rs"*

Approcciando il problema di valutazione della resilienza in un ambiente multirischio, in [1], partendo dalla valutazione delle quattro proprietà (*Robustness, Redudancy, Resourcefulness e Rapidity*) che compongono in paradigma sopra citato, è stata presentata la seguente misura:

$$\psi = \frac{T_i + F\Delta T_f + R\Delta T_r}{T_i + \Delta T_f + \Delta T_r} \tag{2.14}$$

dove, come illustrato in Fig. 2.21 (sotto), per ogni evento di alterazione f ed ogni evento di ripristino r, si distinguono:

- un corrispondente profilo di *Failure (F)* misurato come:

$$F = \frac{\int_{t_i}^{t_f} f \; dt}{\int_{t_i}^{t_f} Q \; dt} \tag{2.15}$$

  il cui valore può essere considerato come una misura di *Robustness* e *Redudancy*

- un corrispondente profilo di *Recovery (R)* misurato come:

$$R = \frac{\int_{t_f}^{t_r} r \; dt}{\int_{t_f}^{t_r} Q \; dt} \tag{2.16}$$

  il cui valore può essere considerato come una misura di *Resourcefulness* e *Rapidity*

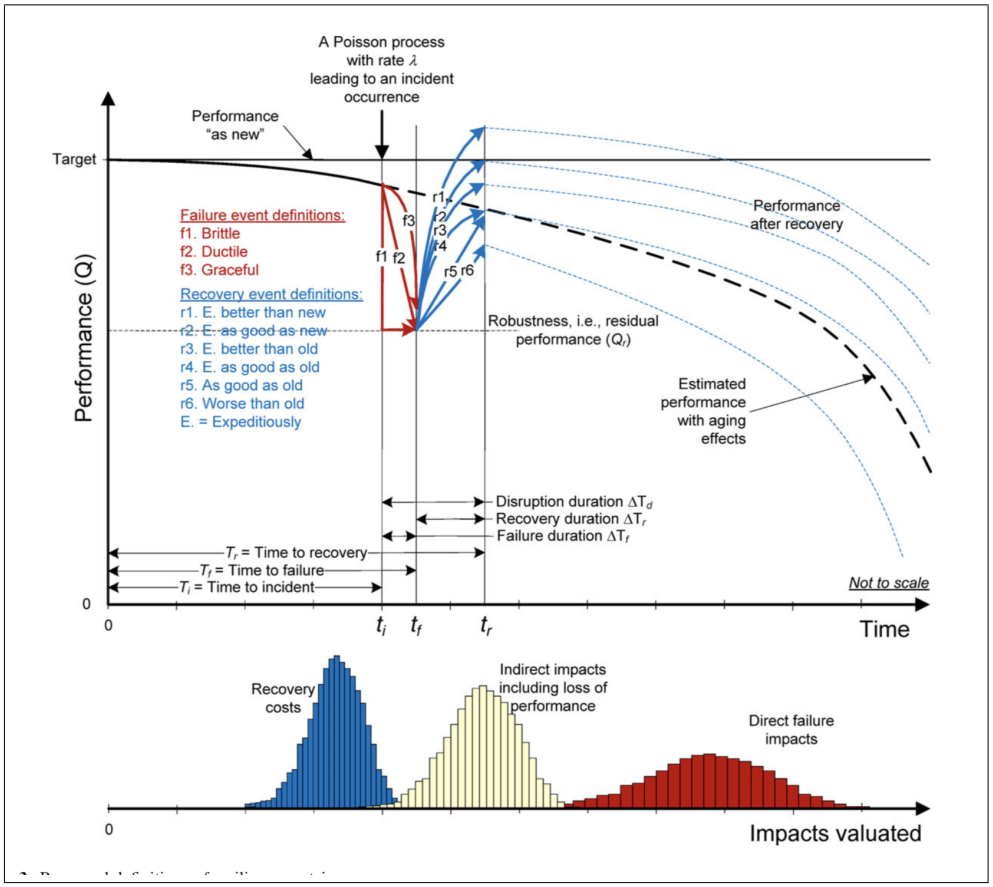

Figura 2.21: Descrizione profili, proprietà e parametri dell'eq.ne 2.14 [1]

N.B.: Il grafico della curva di performance (Q) sopra illustrato suggerisce anche una possibile valutazione in termini probabilistici del *time to failure* (T_f) considerando gli effetti di invecchiamento del sistema ed evidenziandone la loro incidenza nel tempo, sia nella fase *pre* che *post-disruption*.

Considerando che la misura di resilienza sopra identificata può essere utilizzata per qualsivoglia tipo di sistema (i.e. impianti, infrastrutture, reti e comunità), in [41], è proposto un utilizzo dell'indice di resilienza R_i, nel range $[0, 1]$, per ogni i-esimo indice di prestazione e, sull'assunzione della loro indipendenza, è formulata (nel caso di due indici) la seguente formula di aggregazione:

$$\psi_{12} = \frac{R_1 R_2}{R_1 + R_2 - R_1 R_2} \tag{2.17}$$

A supporto della proposta di valutazione aggregata della resilienza di sistema, in Fig. 2.22, sono presentate (sulla base delle differenti tipologie di sistema) alcune possibili misure di performance utilizzabili e le lore relative unità di misura.

Systems	Performance	Units
Buildings	Space availability	Area per day
Other structures: Highway bridges	Throughput traffic	Count per day
Facilities: Water treatment plants	Water production capacity	Volume per day
Infrastructure: Water delivery	Water available for consumption	Volume
Network: Electric power distribution	Power delivered	Power per day
Communities	Economic output	Dollars
Communities	Quality of life (consumption)	Dollars

Figura 2.22: Misure di performance per sistema [1]

A conclusione della classificazione presentata, in Fig. 2.23 (sotto), è proposta una tabella riepilogativa di confronto tra le misure quantitative di resilienza individuate e la totalità delle peculiarità e/o paradigmi utilizzati per la loro quantificazione.

OSSERVAZIONE: Lungo la diagonale della sottomatrice 5x5 (evidenziata in rosso) ogni gruppo di indici proposti (a sx) incrocia le proprietà (o il paradigma) utilizzato per la sua definizione.

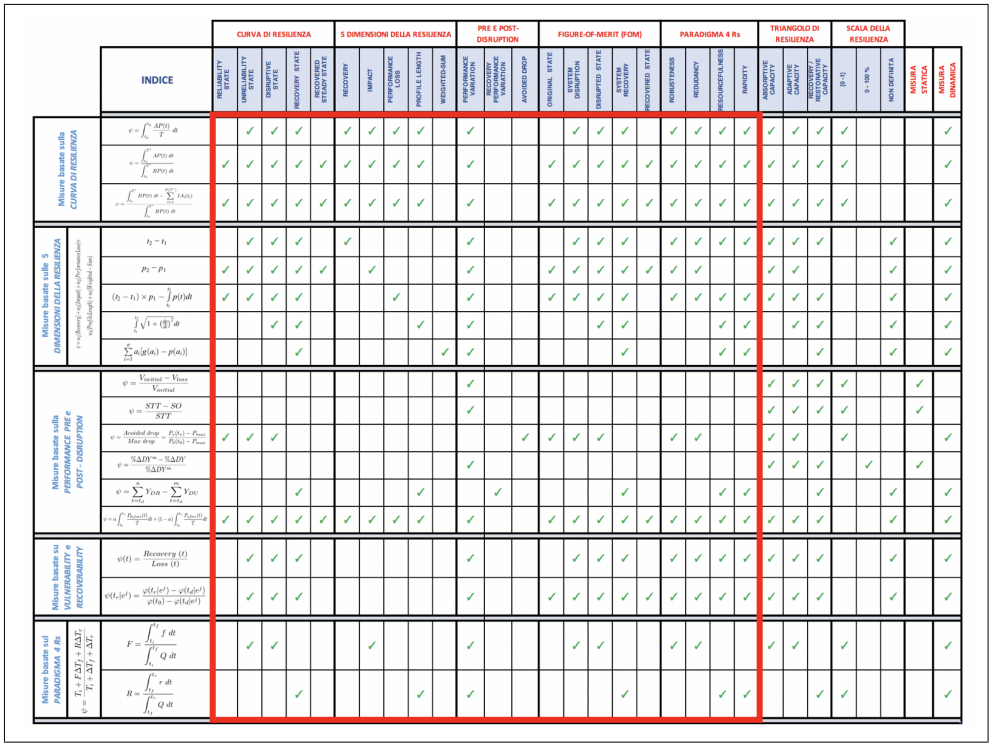

Figura 2.23: *Misure generiche di resilienza* vs *proprietà e/o paradigmi* utilizzati per la loro definizione